

What is claimed is:

1. A device for calculating a result of a modular exponentiation, n being a modulus, d being an exponent and
 5 c being a quantity to be subjected to the modular exponentiation, comprising:

means for calculating a first auxiliary quantity dp,
 wherein dp is defined as follows:

10

$$dp = d \bmod (p - 1),$$

wherein p is a first prime number;

- 15 means for calculating a second auxiliary quantity dq,
 wherein dq is defined as follows:

$$dq = d \bmod (q - 1),$$

- 20 wherein q is a second prime number,

wherein a product of p and q equals the modulus n;

means for generating a random number (IRND);

25

means for generating a third auxiliary quantity dp',
 wherein dp' is defined as follows:

$$dp' = \text{IRND} \times (p - 1) + dp;$$

30

means for generating a fourth auxiliary quantity dq',
 wherein dq' is defined as follows:

$$dq' = \text{IRND} \times (q - 1) + dq;$$

35

means for generating a fifth auxiliary quantity Mp, wherein
 the fifth auxiliary quantity Mp is defined as follows:

$$M_p = c^{dp'} \bmod p;$$

means for generating a sixth auxiliary quantity M_q , wherein
 5 the sixth auxiliary quantity M_q is defined as follows:

$$M_q = c^{dq'} \bmod q; \text{ and}$$

means for calculating the result of the modular
 10 exponentiation m , wherein m is defined as follows:

$$m = M_q + [(M_p - M_q) \times q^{-1} \bmod p] \times q.$$

2. The device according to claim 1, further comprising
 15 means for generating a safety parameter T ,

wherein the means for generating the fifth auxiliary
 quantity M_p is formed to calculate the fifth auxiliary
 quantity as follows:

20

$$M_p = c^{dp'} \bmod (pT), \text{ and}$$

wherein the means for generating the sixth auxiliary
 quantity M_q is formed to calculate the sixth auxiliary
 25 quantity M_q as follows:

$$M_q = c^{dq'} \bmod (q \times T).$$

3. The device according to claim 2, further comprising
 30 means for calculating a seventh auxiliary quantity H_7 ,
 wherein the seventh auxiliary quantity H_7 is defined as
 follows:

35

$$H_7 = M_p \times M_q \bmod T, \text{ and}$$

wherein means for calculating an eighth auxiliary quantity H8 is further provided, wherein the eighth auxiliary quantity H8 is defined as follows:

$$5 \quad H8 = c^{(dp' + dq') \bmod (T-1)} \bmod T; \text{ and}$$

means for comparing the seventh and eighth auxiliary quantities, wherein the means for comparing is arranged to indicate a fault when the seventh and eighth auxiliary quantities differ.

4. The device according to claim 1, being provided for an RSA decryption or RSA signature, m being a plain text message, d being a secret key and c being an encrypted message.

5. A device for calculating a result of a modular exponentiation, n being a modulus, d being an exponent and c being a quantity to be subjected to the modular exponentiation, comprising:

means for calculating a first auxiliary quantity dp, wherein dp is defined as follows:

$$25 \quad dp = d \bmod (p - 1),$$

wherein p is a first prime number;

means for calculating a second auxiliary quantity dq, wherein dq is defined as follows:

$$dq = d \bmod (q - 1),$$

wherein q is a second prime number,

wherein a product of p and q equals the modulus n;

means for providing a safety parameter T ;

means for generating a third auxiliary quantity $p \times T$ and a fourth auxiliary quantity $q \times T$;

5

means for generating a fifth auxiliary quantity M_p , wherein the fifth auxiliary quantity M_p is defined as follows:

$$M_p = c^{dq} \bmod (p \times T);$$

10

means for generating a sixth auxiliary quantity M_q , wherein the sixth auxiliary quantity M_q is defined as follows:

$$M_q = c^{dq} \bmod (q \times T); \text{ and}$$

15

means for calculating the result of the modular exponentiation m , wherein m is defined as follows:

$$m = M_q + [(M_p - M_q) \times q^{-1} \bmod p] \times q.$$

20

6. The device according to claim 5, wherein the safety parameter T is a prime number.

7. The device according to claim 3, wherein the safety parameter T is small compared to the first prime number p and the second prime number q , respectively.

25

8. A method for calculating a result of a modular exponentiation, n being a modulus, d being an exponent and c being a quantity to be subjected to the modular exponentiation, comprising the following steps:

30

calculating a first auxiliary quantity d_p , wherein d_p is defined as follows:

35

$$d_p = d \bmod (p - 1),$$

wherein p is a first prime number;

calculating a second auxiliary quantity dq , wherein dq is defined as follows:

5

$$dq = d \bmod (q - 1),$$

wherein q is a second prime number,

10 wherein a product of p and q equals the modulus n ;

providing a random number (IRND);

generating a third auxiliary quantity dp' , wherein dp' is defined as follows:

15

$$dp' = \text{IRND} \times (p - 1) + dp;$$

generating a fourth auxiliary quantity dq' , wherein dq' is defined as follows:

20

$$dq' = \text{IRND} \times (q - 1) + dq;$$

generating a fifth auxiliary quantity Mp , wherein the fifth auxiliary quantity Mp is defined as follows:

25

$$Mp = c^{dp'} \bmod p;$$

generating a sixth auxiliary quantity Mq , wherein the sixth auxiliary quantity Mq is defined as follows:

30

$$Mq = c^{dq'} \bmod q; \text{ and}$$

calculating the result of the modular exponentiation m , wherein m is defined as follows:

35

$$m = Mq + [(Mp - Mq) \times q^{-1} \bmod p] \times q.$$

9. A method for calculating a result of a modular
 exponentiation, n being a modulus, d being an exponent and
 c being a quantity to be subjected to the modular
 5 exponentiation, comprising the following steps:

calculating a first auxiliary quantity dp , wherein dp is
 defined as follows:

$$10 \quad dp = d \bmod (p - 1),$$

wherein p is a prime number;

calculating a second auxiliary quantity dq , wherein dq is
 15 defined as follows:

$$dq = d \bmod (q - 1),$$

wherein q is a second prime number,

20

wherein a product of p and q equals the modulus n ;

generating a safety parameter T ;

25 generating a third auxiliary quantity $p \times T$ and a fourth
 auxiliary quantity $q \times T$;

generating a fifth auxiliary quantity Mp , wherein the fifth
 auxiliary quantity Mp is defined as follows:

30

$$Mp = c^{dp} \bmod (p \times T);$$

generating a sixth auxiliary quantity Mq , wherein the sixth
 auxiliary quantity Mq is defined as follows:

35

$$Mq = c^{dq} \bmod (q \times T); \text{ and}$$

calculating the result of the modular exponentiation m ,
wherein m is defined as follows:

$$m = Mq + [(Mp - Mq) \times q^{-1} \bmod p] \times q.$$